Computer Security Administrative Procedure

-- DRAFT --

Updated July, 2003
Department of Technology Services

Table of Contents

1. SCOPE

The scope of this Administrative Procedure document includes all County owned or controlled computers (PCs, laptops, PDA's, servers, mini-computers, mainframe computers), all County owned or leased buildings, all data stored on those devices, all printouts, disks, tapes, or other media produced by those devices and all licensed software used on those devices. In addition, this Administrative Procedure includes communications links to contractors and business partners and extensions of the County's computer network.

This Administrative Procedure applies to all County employees, contractors, volunteers and persons legitimately affiliated with the County government for the efficient exchange of information and the completion of assigned responsibilities.

2. OVERVIEW

This Administrative Procedure statement reflects accepted security controls taken from respected security and audit publications and adapted to Montgomery County's technical environment. These data security policies and standards have been developed to protect Montgomery County Government's electronic data assets from theft, destruction, and unauthorized use, modification, or disclosure. Security policy must be in compliance with all relevant federal and state laws. The loss of these assets could be very costly and disruptive to the County government. In today's computing environment, security controls are a necessity. The citizens of this County will expect us to do what is prudent to protect the computing assets purchased with their tax dollars. Data is one of the most valuable assets of the County government. End-user computing dramatically increases the exposure for theft, corruption, loss, and misuse of County information resources since a significantly larger number of people have access to data and data security controls. A significant percent of direct access storage device capacity is installed outside the Computer Center. Security is an issue that cuts across all computing and organizational tiers. The implementation of security policies and procedures requires cooperation among users, managers, information systems personnel, security and audit personnel and top management.

Access to the entire County's computing and communication resources is to be controlled based on the needs of the County and used for official County business only. Connection and access to computing resources is controlled through unique user identification (user-ids) and authentication (passwords). Each individual granted this privilege is responsible and accountable for work done under their unique identifier.

Computer users will be given access to a copy of the latest version of this Administrative Procedure and the *Internet, Intranet, & Electronic Mail Administrative Procedure*. Individuals must adhere to the policies and are responsible for having the latest version of the Administrative Procedure. Refer to the *Internet, Intranet, & Electronic Mail Administrative Procedure* for additional information related to use of the Internet.

3. RESPONSIBILITIES

All Montgomery County Government computing and communication hardware, software, and data is considered to be "owned" by the Montgomery County Government.

The Department of Technology Services (DTS), in accordance with Montgomery County code section 2-58D, is responsible for protecting the integrity of the telecommunications network backbone, for operation and maintenance and security administration of the "enterprise" servers, mainframe and for maintaining this Administrative Procedure statement. DTS is responsible for insuring that computer connections between County departments and with other government agencies are accomplished securely and as authorized.

Management in each department is responsible for ensuring that these computer security controls are enforced on the computing resources in their department. These security controls will be enforced for employees as well as for contractors and volunteers. Department management is responsible for providing pertinent information and notifying the DTS Security Team if a serious security breach occurs such as an intrusion, theft, or damage of computing resources. The operation, maintenance and security of de-centralized computing resources is the responsibility of department management in accordance with security policy and other policies, as appropriate. A department must make this procedure a part of any contract in which the County is to provide the contractor or its agents or its employees or volunteers, access to County computing resources,

The Local Area Network (LAN) administrator or decentralized IT staff is responsible for implementing the computer security controls described in this document on the servers in their department. LAN administrators will contact DTS network management for allocation of IP addresses.

As a user of data or computing resources or a custodian of those assets, everyone is responsible for data security. County employees who violate this administrative procedure may be subject to disciplinary action, in accordance with Montgomery County laws and executive regulations, including Personnel laws, regulations, and Ethics Laws, currently codified at Chapter 33, Appendix F, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended. Violation of this procedure is prohibited and may lead to disciplinary action, including dismissal, and other legal remedies available to the County.

4. PHYSICAL SECURITY

4.1 Policy:

Physical access to servers, individual PCs, and minicomputers will be protected from unauthorized persons. Personnel will not be put at risk of bodily harm.

4.2 Environmental Requirements and Recommendations:

A safe environment must be provided. Fire detection and suppression, and power and air conditioning are examples of the computer environmental protection and safety systems that must be provided.

- Areas with critical computer equipment must be equipped with fire and smoke alarms, and fire extinguishers.
- Critical equipment should be stored in a location that minimizes or prevents water damage due to leaking or flooding.
- Tall and top-heavy items must be stored in a manner anchored at to prevent damage or physical tipping.

- Items on wheels must have locking mechanisms to prevent rolling.

All equipment is to be maintained in a clean environment that meets or exceeds the manufacturer specifications related to temperature and humidity. Equipment areas should be kept free of obstructions. The cleanliness, environmental protection and safety systems are to be regularly monitored, and periodic inspections by qualified personnel should be scheduled. Electrical protection must be provided. Computer systems should have uninterruptible power supplies (UPS) and/or surge suppressors. All electrical wiring must meet state and local building codes. Preventive maintenance on computer and communications must be regularly scheduled. Preventive maintenance as defined by the manufacturer will help ensure that the risk of failure is minimized.

All new computer or communications centers must be located in an area unlikely to experience natural disasters, serious or man-made accidents, and related problems. New and remodeled facilities must be constructed to protect against fire, water damage, vandalism, and other threats that may occur. The location of multi-computer or communications facilities should be selected to minimize risk of damage. Locating such facilities above the ground floor will minimize the chances of water damage and theft. Kitchen facilities also must be located away from, but not directly above or below computer facilities. Due to potential water damage, restroom facilities should not be located directly above these facilities. Computer facilities should not be located adjacent to an exterior wall to protect the systems from unauthorized electromagnetic eavesdropping and damage from bombs.

DTS can provide the needed facilities more economically than creating a new computer center. If a new computer center needs to be created, contact the manager of the DTS computer center for requirements assistance. Local laws and ordinances must be considered when designing these locations.

4.3 Access to Work Areas:

Access to all buildings, computer labs, offices, and work areas containing computer-related equipment must be physically restricted and controlled. Access to servers and wiring closets must be restricted. Only authorized personnel will have access to wire closet/server areas. Authorized persons may include:

- DTS staff
- Outside contractors hired to work in these areas
- Building services and office staff at locations trained to reset equipment
- Fire and/or rescue personnel

Access to computer equipment must be supervised. Access to offices, computer rooms, and work areas containing sensitive information must be physically restricted. Managers responsible for employees working in these locations must determine the appropriate access controls. All multi-user computer and communications equipment such as fileservers, labs, and wiring closets must be located in locked rooms to prevent unauthorized usage.

Access to Server Centers or Network Operations Centers (NOCs) is restricted. Only employees whose job responsibilities require access to the client server center will be granted access. The supervisor of a server center or NOC is responsible for authorizing entrance and maintaining a list of those authorized to enter the facility.

Access to magnetic tape, disk, and documentation libraries must be restricted to employees whose responsibilities require access to them. The magnetic tape, disk, and documentation libraries housed within the controlled areas of the Server Center require additional precautions. This access is controlled by the supervisor of the Server Center. Employees are not to permit unknown or unauthorized persons to enter restricted areas as they enter and exit these areas. Physical access controls for County buildings are intended to restrict the entry of unauthorized persons, and employees are expected to help restrict such access.

4.4 Removal of Equipment:

Permission to remove computers or related equipment may be granted only for accepted business purposes. Permission to remove computer equipment must be approved by the director of the department owning the equipment and the reason for lending the equipment must be put in writing stating the reason for which the equipment is loaned. Equipment being removed for needed repairs has implied permission when DTS approved repair processes are followed and a receipt is retained for the equipment.

PC equipment must not be moved or relocated without prior authorization from the appropriate management and/or DTS technical support staff. PC workstations, printers, peripherals, file servers, and electronics are examples of PC equipment covered by this requirement.

All County property must be returned when employees, consultants, or contractors terminate their relationship with County or with a specific work location within the County. It is the responsibility of the supervisor to collect County property from an employee leaving their location. Personnel terminating County employment or moving from one work location to another must inform their supervisor/administrator regarding County property they possess, and building access privileges.

When a computer support employee is involuntarily terminated, due care must be taken. Upon involuntary termination, the employee is to be immediately relieved of all duties and must return all County equipment and information. Their network accounts are to be immediately disabled and they are to be supervised while packing their belongings and leaving County facilities.

A sign-out procedure, approved by department management, must be utilized for laptop computers if there is a shared pool of laptops.

Montgomery County is not responsible for maintenance, damage or loss of personally owned computers or peripherals in the work place.

4.5 Personnel Security

Employees should contact building security if they feel threatened, harassed, or afraid of bodily harm.

Personnel will immediately contact building security if a person:

- becomes unruly
- refuses to leave
- poses a threat to employees, property, or equipment

In the case of an emergency, Montgomery County Police should be immediately contacted or dial 911. This is judgment decision based on the severity of the threat. If in doubt, contact the police first then building security

4.6 Disaster Recovery

A detailed disaster recovery plan must be developed by each department that has a LAN or mini-computer. This plan will detail procedures to follow in the event of the loss of computing hardware, software and/or data. DTS must prepare, periodically update, and regularly review information technology emergency response plans for the DTS data center and for communications systems. The disaster recovery plan must provide for the continued operation of critical systems in the event of an interruption or degradation of service; must allow all critical computer and

communication systems to be available in the event of a major loss, such as a flood, earthquake, or tornado; must prioritize the sequence of critical systems being recovered. This plan must be practiced at least once a year; this practice will include restoring data from backup media to insure that restoration procedures are known and to verify the integrity of the backup media. Each test must be followed by a report, and detail the test results, plus any remedial actions taken. The department can evaluate the effectiveness of the plan and make adjustments as appropriate to accomplish the desired goals. The manager of the DTS data center can provide a comprehensive sample of a disaster recovery plan

A business continuity analysis will also be conducted by those responsible for their department computing equipment that identifies the procedures that need to be in place in order to ensure that critical operations could continue in the event of a disaster which destroys their computing capabilities. The conditions that warrant a disaster declaration and the persons responsible for this decision will be specified.

Departments wishing to be supported by the DTS in the event of an emergency or disaster must implement hardware, software, policies, and related procedures consistent with DTS standards. DTS staff is available to work with offices to ensure compliance with DTS standards. Refer to http://portal.mcgov.org/security/ for disaster recovery steps to be taken by departments not supported by DTS.

Backup medium must be erased by following the *Data Backup* section in this Administrative Procedure.

The communications networks should be designed without a single point of failure whenever possible, such as a central switching center, which could affect the availability of network services.

A backup of system wide critical information and software is to be stored in a physically separate, environmentally controlled facility. This facility is to be at least five miles from the site where original copies reside. Additionally, all current supporting materials such as manuals, charts, and diagrams needed for disaster recovery will be housed at the same facility. Supporting materials include anything required by County departments or units that are necessary to maintain day-to-day mission critical operations until recovery. Contact the DTS data center manager for information on the facility used by the data center for backups.

4.7 Emergency Shutdown Procedures

A detailed plan will be developed by each department with their own LAN or Mini-computer to shut down each device in a computer center quickly in the event of an emergency. Emergencies can include fire, loss of environmental controls, computer virus outbreak, natural disasters, etc. The goal is to preserve County resources in an emergency without subjugating the operator to undue risk. Contact the DTS data center manager for a sample of this plan. The DTS security manager or the director of the affected department can make this determination and contact the appropriate department management personnel to implement the emergency shutdown procedures when warranted by the circumstances. This kind of emergency will require every effort to shut down the computing equipment. Unplug the equipment from the County network if shutdown is not possible.

5. DATA SECURITY

5.1 Policy

Employees that are permitted access to computer systems must follow guidelines in order to insure that restricted access is maintained. Users of the computer systems will only have the minimal access needed to perform their tasks. Attempts to bypass security procedures to gain unauthorized access to computer resources are unacceptable and may result in disciplinary action. See section 3 paragraph 5 for information regarding disciplinary action.

5.2 Password and user-id Information:

Meaningful passwords will be used to protect access to County networked computer systems (LANs, mini-computers, PCs. Unused and default or installation user-ids will be disabled. Use of powerful user-ids such as those with system administrator attributes will be restricted.

Passwords provide a basic first-level security for restricting access to computer resources. To protect County computer resources properly, passwords are required to access all networked computer systems. Passwords will be simple enough to memorize but unique enough to remain secret. Passwords will not be attached to a terminal or other public place where they are easily compromised. Passwords will not be associated with the current date or a person's name, hobby, or family. Good passwords are not found in the dictionary, contain numeric as well as alphabetic characters, and will be at least eight characters in length. Passwords will not be imbedded in user's automatic sign-on procedures unless approved by that department's management for procedures where it is required. Passwords cannot be changed in less than 2 days.

A maximum of ninety days between password changes is required for network, server and mini-computer access. The change interval for power on passwords for PCs, if used, is at each department's discretion. Where possible, password change will be controlled automatically by security software. Passwords will be individually maintained to ensure confidentiality and individual accountability. Passwords will not be shared with others. If multiple people must share a user-id and password for a sound business reason, refer to the exception procedures in section 8 of this document. If it becomes necessary to give your password to a technical person to fix a problem you are experiencing, the password will be changed immediately after the problem is solved. An account will be suspended after no more than five invalid password attempts in a given day and remain suspended until an administrator can reactivate it. Passwords will not be reused for at least four password cycles. A user-id will be suspended after twelve months of non-use.

Access to computer resources will be terminated immediately for employees who leave County employment or when their responsibilities no longer require them to access those resources. Access will also be terminated immediately for contractors no longer requiring access to County computer resources. Department coordinators are responsible for deleting user-ids of people who have terminated, transferred out of the department, or no longer require computer access. If the department coordinator does not have access rights in order to remove or disable the account, then the coordinator must contact the DTS Security Office and E-messaging Directory Services Team.

Computer system security will prevent a user-id from being logged on in more than two different places at the same time. Just one user-id per computer platform will be assigned to an individual. System privileges, such as supervisory or system administrator attributes are sensitive and are restricted to designated LAN or minicomputer system administrators. When the use of sensitive system privileges is necessary by others (for example, during an on-site visit by field service engineers), the privilege will be immediately removed or the user-id disabled after the user is finished with the specific task.

DTS will test password quality on a periodic basis. If a password is found to be weak, the user will be required to change it.

5.3 Protection of Sensitive Information

Sensitive information includes criminal justice, payroll/personnel, client or patient information and any other data considered confidential by law or departmental policy. Sensitive information will not be stored on a PC unless PC security software has been installed on that PC. Sensitive information should be stored on the mainframe or network server where better security is available to protect the integrity of this information. Access to this information will be restricted to those who have to use it. Examples of information that will be protected from unauthorized access include: word processing documents containing sensitive material, which can be locked (password protected); source code for programs, which can be protected using a source code management tool; databases, which can use built-in security controls; and production files downloaded from the mainframe or server, which can be protected in a directory where limited access is permitted.

Sensitive information stored on computer diskettes, tapes or printout will be locked in a secure area when not in use and deleted, reformatted or shredded when no longer needed.

The same level of security will be maintained across the various computer platforms (mainframe, mini, LAN or individual PC). If a sensitive file located on the mainframe computer is downloaded to an individual PC, that information on the PC will be protected from unauthorized access in an equivalent manner as it is on the mainframe.

PC's and terminals will not be left unattended with the results of a query containing sensitive information displayed on the screen. If this is necessary, a screen locking feature that blanks the screen until the correct password is entered will be used. Sensitive printouts will not be left on an unattended printer.

Special care will be given for laptop or portable PC's. If possible, sensitive information will be stored on diskettes rather than the hard drive and in a separate secure location from the laptop. Some sensitive information may need to be encrypted in order to ensure adequate security. A power on password will be used. If the PC is lost or stolen, departmental security personnel and the DTS Security Team will be notified immediately, and a complete accounting of what was on that PC will be made.

If possible, unauthorized attempts to access sensitive information will be logged and kept for a period of at least one year. This is information that may be used as evidence in a criminal proceeding and must be protected.

Do not disclose user-ids, passwords or other sensitive information to anyone without verifying their authorization to have this information.

The following statement is wording approved by the County Attorney's Office that will be displayed to users before they are granted computer access. This warning banner will appear each and every time that someone logs into a County computer:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device.

5.4 Data Backup:

Data and files that are crucial to the department's operations will be backed up and the retention of at least the last three copies is highly recommended. The frequency of backup is to be commensurate with the frequency of change and the criticality of recovering the lost data in a timely manner. Some data may need to be backed up daily; monthly backups in other cases may be sufficient. When possible, backups will be automated and take place during off-peak hours.

All archival back-up data that is stored off-site must be listed in a current log that shows the date when the information was last modified, as well as the content of the information. All media used to store sensitive, valuable, or critical information for longer than six months must not be subject to rapid degradation. This information must be copied to newer media when the time limits suggested by the manufacturer are exceeded.

Offsite storage facilities will be utilized for copies of backup files containing programs, data or transactions representing current County business that, if lost or destroyed, would be difficult or impossible to recreate. All backups will be retained a minimum of four weeks and at least two copies will be kept in offsite storage. Longer retention periods should be considered based on business requirements. Offsite storage facilities will also be utilized for files containing data with retention requirements imposed by county, federal or state government. Magnetic storage media provided by the offsite storage or disaster recovery facility for the purpose of restoring Montgomery County information will be thoroughly erased after being used. This may be done by programs designed to erase sensitive information or by reformatting the media at least 7 times.

Additional protections, such as mirror disks, RAID technology, and hardware redundancy should be used as appropriate for mission critical applications. Contact the DTS data center manager if you need assistance in setting up backup/restore procedures or need offsite storage procedures

5.5 Virus Control

Virus controls are necessary to prevent the spread of computer viruses to other computers in the network. Virus eradication can be very time consuming and result in the loss of service to the citizens of Montgomery County.

Software not purchased by the County (e.g. software from bulletin boards, software from home computers or any other computer or network), when allowed by County and department policy, will be checked for viruses before use. This includes diskettes, CD-ROMs and information downloaded from the Internet or other on-line services. Information downloaded to the hard drive will be checked immediately upon completion of the download. Diskettes and CD-ROMs received from other departments or agencies or from companies doing business with the County will be checked before use.

All those responsible for departmental computer resources will update those resources with anti-virus signatures on a minimum weekly basis and upgrade to the most current anti-virus release as it becomes available. All PC's and servers that are connected to the county network must have DTS approved, centrally administrated anti-virus software installed and running using a DTS approved configuration. Automatic updates will be utilized if available. Contact the DTS Client Computer Services (DCM) if information is needed on anti-virus software. When DTS issues a security alert and specifies that virus signatures must be updated immediately, those responsible for departmental computer resources must comply.

5.6 Software Security Upgrades

Vendors publish patches and upgrades to their software when they discover security flaws that could allow computer security to be compromised. The DTS Security Team may provide information about enterprise software security issues and patches as available and appropriate.

Because these flaws pose a significant threat, critical security patches for internal computer systems must be applied in a maximum of 30 days after public release. For systems containing sensitive information or are accessible via the Internet, critical security patches must be applied within 7 days of public release. Automatic updates will be utilized if available. If alerted of a specific critical threat that could severely affect County resources, the DTS Security Office may issue a mandatory, short time frame alert to computer administrators to patch specific computer resource in order to reduce the risk of network down time.

Non-critical security patches must be applied to all systems within 90 days of public release.

If, due to incompatibility or other issues, a critical security patch cannot be applied, an exception report must be sent in writing to the DTS Security Office.

On a regular basis, the DTS Security Office will verify software revision and patch levels for all County systems. Refer to the *Vulnerability Assessment and Remediation* section for details.

6. NETWORK SECURITY

6.1 Policy:

Access to or from the County network is only permitted for authorized employees and other County approved agencies.

6.2 Remote Dial-in Access to County Computer Resources:

Access to remote network services will be in accordance with the *Internet, Intranet, & Electronic Mail Administrative Procedure*. Approval from the department management and the DTS Security Office will be obtained if a user requires a modem at their workstation for remote access. Modems attached to PC's that are connected to a County network can be very risky and will not be authorized unless DTS-approved security measures are implemented. Unauthorized modems attached to PCs or servers that are connected to a County network are prohibited. If remote access from a County owned PC using an attached modem is required, that PC will be disconnected from all LANs or networks. Refer to the *Internet, Intranet, & Electronic Mail Administrative Procedure* document.

6.3 Access from Remote Networks to County Computer Systems

Access from a remote site to any Montgomery County computer resource will be approved by the employee's Department head or designee and by the DTS Security Office. All remote access systems used to access County computing resources will be approved by the DTS Security Office prior to purchase, installation, or connecting to County resources. Access and security system information must not be disclosed to any 3rd party.

Employees who need remote access to any County computer resources will submit a request in writing to the DTS Security Office stating what the access is to be used for, how long the access is required, and approval from the responsible department official. Employees working from home can refer to the Telecommuting Policy in http://portal.mcgov.org/Itintra/PolicyProcs/polproc.html. Contact the DTS Security Office to obtain information and approval for secure remote access options including, but not limited to, RAS, VPN, and wireless methods. Modems

attached to County computer systems that allow remote access is not an approved remote access method. The list of authorized remote access users will be reviewed periodically by the LAN or mini computer administrator to determine continued need for such access and accuracy of the list. If remote access is no longer required, that access will be terminated.

LAN and mini computer administrators will maintain a log of unsuccessful attempts to access County computers. This log will be maintained for one year.

Encryption of any County-owned data is required if it is to be transmitted over public phone lines, the Internet, or wirelessly. County approved remote access solutions already use encryption.

6.4 Contractor Remote Access

All contractors will meet the same security requirements detailed in this and all other related County documents. The contractor will agree to, and is responsible for, maintaining compliance with all County security policies. Virtual Private Network (VPN) is the current approved remote access method. The sponsoring Department head or designee and the DTS Security Office will approve the remote access request.

The department whose contractor requires remote access to the County's network will present a written justification to the DTS Security Office. All plans for establishing remote access will be approved by the DTS Security Office in advance of implementation. These plans will include at least the following:

Type of access
When and how long access will be required
Security procedures (how contractor access will be controlled)

All contractors requiring access will sign non-disclosure statements and agree to abide by all County security policies and procedures prior to receiving access.

6.5. Extended Networks

Extended Networks are permanent or semi-permanent physical extensions of the County's computer network to a non-County facility and used by non-County employees to access County computer resources.

All network extensions to a contractor or business partner facility will meet the same security requirements detailed in this and all other related County documents. The Contractor/Business Partner (C/BP) will agree to, and is responsible for, maintaining compliance with all County security policies.

The Department requesting the extended network will present a written justification to the DTS Security Office for granting a C/BP access to the County's network from a remote location.

The C/BP will provide a secure link (e.g., T-1) between the C/BP site and the County's Computer Center. All plans for establishing a link will be approved by the DTS Security Office in advance of installation. These plans will include the following:

Type of connection
How long connection will be required
Hours of operation
Number and type of workstations and servers at remote location

Physical security plan
Security Procedures (including keeping all security systems up-to-date)
Anti-virus procedures
Whether Internet access is required for any workstations
The process of disconnecting the C/BP once the connection is no longer needed

All material submissions mentioned above will be submitted by the Contractor / Business Partner to the County Department requesting the extended network, which will coordinate reviews and approvals with the DTS Security Office.

The C/BP will maintain all security provisions, detailed in this Administrative Procedure, while the remote location is connected to the County network. All employees that have access will sign non-disclosure statements, receive security training, and agree to abide by all County Security Policies and procedures (sign County security agreement), prior to receiving access. All training materials will be approved by the DTS Security Office in advance.

A list of employees with authorized access will be kept up to date and provided in a monthly report to the DTS Security Office. Requests for additional staff access will be approved by the DTS Security Office or County contract administrator prior to granting the access.

The C/BP will permit the DTS Security Office to inspect the remote location without notice, at any time. This may include technical security scanning of the C/BP network segment and any system connected to it.

The C/BP network segment, defined as all workstations, servers, and network equipment connected to the County, will not also be connected to any other network (including the C/BP own internal network). Remote access to the C/BP network segment will NOT be permitted; dial-in or dial-out will not be allowed.

Failure to maintain full compliance with the County's security policies will result in immediate termination of the connection, and may be cause for cancellation of any contract between the County and the C/BP.

6.6 Vulnerability Assessment and Remediation

System/network administrators need to have a vulnerability assessment performed against their assets on a bi-yearly basis. All aspects of this security Administrative procedure will be evaluated for risk assessment. The security manager will determine the exact schedule. The security manager may also define any additional security assessments other than those described here. In cases where networks reside behind firewalls, multiple assessments should be conducted from both the internal and external sides (or all sides) of the firewalls. Vulnerability assessment information and procedures are posted on the County portal in http://portal.mcgov.org/security/

The security manager will be responsible for conducting scans against common infrastructure. The security manager may also conduct scans at random intervals provided that this activity doesn't interfere with business operations. In cases where loss of services might occur, the security manager will coordinate with the appropriate administrators/authorities prior to the assessment.

System/network administrators will only be allowed to scan segments that they're responsible for. Also, the security manager will determine what signatures and scanning methods will be allowed. If sufficient controls do not exist, then the security manager will conduct a scan on behalf of the administrator.

As a general rule, if a vulnerability assessment reveals high-risk vulnerabilities, administrators will have one week to make appropriate changes. Medium-risk vulnerabilities will be addressed within one month. The security manager

will coordinate with administrators to adjust this timeline as necessary. If no working patch or configuration change exists or if it will cause an extended or re-occurring stop to business operations, the security manager will evaluate any alternatives or provide a waiver. If high risk vulnerabilities are not remediated within the allotted time, the system may be disconnected from the network. In any case, the security manager will be available to assist administrators in developing remediation solutions. Notify the security manager with results of the vulnerability assessment.

All system or network installations must be reported to the security manager prior to implementation. This should include the following:

New or changed network access points (RAS, VPN, wireless, etc.)
New or changed network segments
New or changed business applications
New or changed application/network servers

New installations must meet County Computer Security Administrative Procedure and be scanned for vulnerabilities using tools approved by the DTS Security Office prior to implementation.

6.7 802.11 wireless access

All wireless access points must be approved by the network manager or the security manager. A secure setup on these devices is critical and must be performed by the network team. All other wireless access points connecting to the County network are not permitted. Any existing wireless access points not setup by the network team must be disconnected immediately and the network manager notified to secure the wireless access appropriately.

7. CONDUCT AND USE

7.1 Policy:

County computer systems should only be used in a legal manner for County business.

7.2 Use of County Computer Resources

All use of computer facilities, networks, and technology resources are for County business purposes. Each user of these technology systems is accountable for using these systems responsibility, following all policies, regulations, security requirements, and laws. All new and existing employees, contractors and volunteers will be required to sign a confidentiality agreement.

As such, all electronic mail messages, files on personal computers or servers, or any information stored on or transmitted by County computers are subject to be reviewed, copied, stored, archived, and monitored for violation of policies, regulations, and local, state or federal laws.

7.3 Adherence to Software Copyrights

No unauthorized copies of licensed software may be made or used. It is a violation of copyright and trade secret laws and licensing agreements to make or use unauthorized copies of any licensed software. An inventory of all software will be made periodically to determine if the software is properly licensed. Automated tools such as software metering may be used to ensure compliance with license agreements. If illegal copies of software are found, they are to be deleted from the system immediately or properly licensed to protect the County from litigation. This discovery and deletion will be documented.

Violation of this policy could result in fines to the County by the Software & Information Industry Association and disciplinary action to the employee.

7.4 Security Measures

Users are not to disable or modify security measures installed on any computer for any reason without permission from the appropriate staff. Security measures include such things as menu software, operating systems settings, and anti-virus software. If it is necessary to disable security to perform a hardware or software installation, security measures must be reactivated when installation is complete.

8. EXCEPTIONS

8.1 Policy:

Exceptions to any of these policies or procedures must be approved by the department management and the DTS Security Office. Exceptions will be directed to DTS Security Office by departmental management, in writing or via email, for prompt consideration. A detailed description of the exception will be included as well as the business purpose for this exception and what additional precautions that could be taken to reduce the risk to the County network if the exception is granted. An example of additional security precautions may include restricting internet access and eliminating floppy disk and CD drives on the PC or disconnect from the County network.

There are some older computer platforms in use in the County which lack the capability to implement some of the security procedures outlined in this document. Upgrades or replacements to these computer platforms will be purchased as soon as possible and until this occurs all sensitive information will be moved off these computers. These system exceptions must be documented in writing to the DTS Security Office.

9.0 Policy Updates

9.1 Policy:

The Computer Security Administrative Procedure must be changeable as the need arises. Check at the URL below for guidelines, best practice rules, procedures, and policy updates:

http://portal.mcgov.org/security/

6.0 Security Architecture

6.1 Principles

The Network Security Team uses a wide variety of commercial and open source tools to protect assets from damages resulting from viruses/worms/Trojans and other attacks.

6.2 Components

The following products make up the County's core and initiatives.

Websense

Websense Enterprise Internet Monitoring software enables Montgomery County Government to manage how its employees use the Internet, improving productivity, conserving network bandwidth, and mitigating legal liability. Websense has the ability to block, permit, limit by time-based quota or postpone access to individual categories by user, group, workstation or network.

Websense has several reporting tools to provide risk analysis, productivity reporting and general insight into Montgomery County Government's employees Web usage. The interactive reporting tool provides unlimited views of Web usage information. Real-time Analyzer (RTA) provides Web-based, real-time access to information on network traffic manageable with Websense Enterprise. RTA is an interactive tool for monitoring effectiveness of Web usage policies in real time. Employee Internet Management (EIM) Reporter is a customizable, comprehensive reporting tool that provides detailed information on all Web usage. EIM Reporter may be used to schedule, automatically generate and distribute key information to management.

Nessus Vulnerability Scanners

The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner. The County uses a number of its technologies to identify weaknesses in any hardware device that is connected to the network.

Remote Access - VPN

SmartGate authenticates users, encrypts data and provides flexible access controls for client-to-application security. With SmartGate, Montgomery County Government can securely share critical information and applications with employees and business partners via the Internet. The SmartGate VPN solution is the current approved method for remote access.

Identity and Access Management [Pilot]

The County is currently moving towards a single-sign-on (SSO) architecture. Several technologies have been explored and currently a pilot program to validate the integration of Tivoli Access Manager with the County's Active Directory is underway. The components of the architecture are subject to change pending results of the pilot.

Cisco 4235 IDS

The Cisco IDS 4200 series appliance sensors are purpose-built, high-performance network security "appliances" that protect against unauthorized, malicious activity traversing the network, such as attacks by hackers. Cisco IDS sensors analyze traffic in real time, enabling the County to quickly respond to security breaches. Detection techniques include stateful pattern recognition, protocol parsing, heuristic detection, and anomaly detection, which provide comprehensive protection from a variety of both known and unknown cyber threats.

Log Correlation and Forensics

A Log Correlation and Security Event Management software provides a comprehensive, coherent view of enterprise security. It correlates event data files from disparate machines such as firewalls, intrusion detection systems, computer systems and routers and automatically analyzes this data to uncover legitimate threats to the enterprise. It allows security analysts in Montgomery County to prioritize their investigations and focus on the mission-critical task of responding to threats as they are occurring, rather than after the damage is done. With the software a security team can manage security threats from early detection to final resolution without ever leaving the intuitive, web-based console.

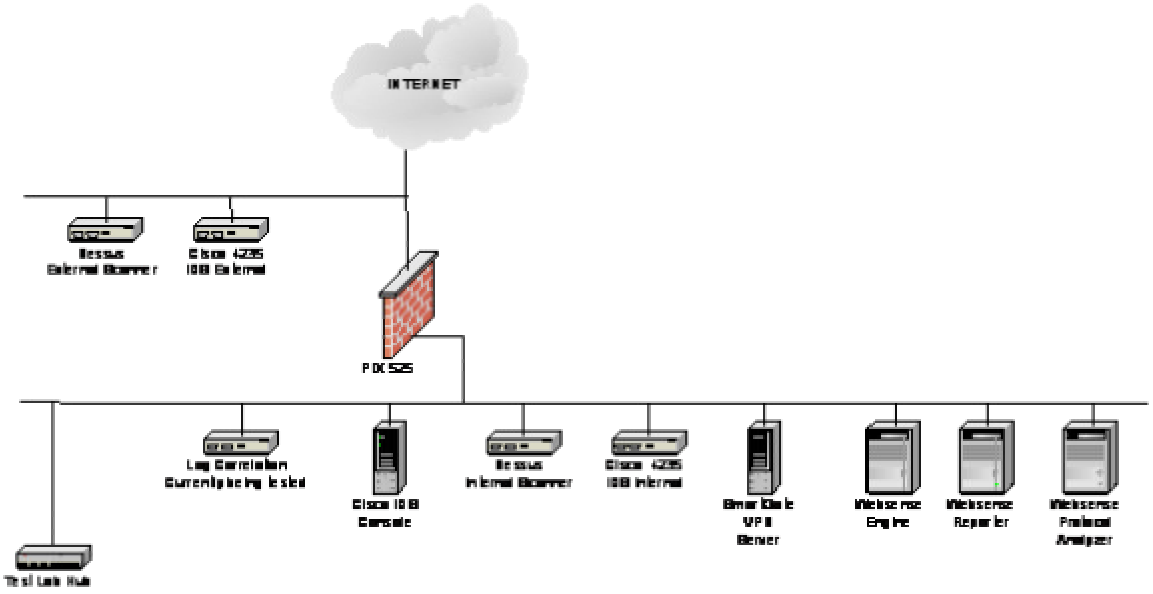

Figure 8 Security Architecture

6.2.1 In-house Competency/Skill Set

In order to maintain the architectural components, DTS personnel will be trained for proficiency in the certain key areas, in order to maintain a high level of service and component availability. Table below captures the required skill sets.

#	Skill Set
1.	Network administration – Routers, Firewall , VPN, Protocols
2.	Network, Server and Desktop Administration. Installation and Troubleshooting
3.	WAN Hardware Management
4.	IDS Administration, Penetration Testing, Vulnerability Assessment and Remediation. Forensic analysis Exploitive techniques